2-6-2022

Conflict and Compromise Over U.S.-E.U. Data Flows

Lydia Balestra

CONFLICT AND COMPROMISE OVER U.S.-E.U. DATA FLOWS

Lydia Balestra

Businesses and other entities that need to make transatlantic cross-border data transfers have waited with bated breath over the past year for a new agreement, after the Court of Justice of the European Union ("CJEU") invalidated a European Union ("E.U.") agreement with the United States that made such data transfers legally possible. Negotiations to develop a long-term, reliable solution are being conducted through the new U.S.-E.U. Trade and Technology Council ("Trade and Technology Council"), which met in Pittsburg, PA, in September 2021.[1] Organizations ranging from Google to the U.S. Chamber of Commerce have stressed the urgency of finding a replacement.[2]

A cross-border data transfer is any transfer of personal data that has been processed or is intended for processing to a third country.[3] The General Data Protection Regulation ("GDPR") restricts cross-border data transfers for the purpose of foiling attempts to undermine its protections by transferring data out of the E.U. The GDPR applies to any personal data that is processed through automated means or is intended to form part of a filing system, and reaches entities established in the E.U. as well as data subjects within it. Because of this, cross-border transfers have wide ranging business applications and are crucial to international organizations.[4]

For cross-border transfers to be permissible, the GDPR requires the transferor to take additional compliance measures, most of which are fairly onerous.[5] By far the most straightforward approach is to make the transfer pursuant to an adequacy decision, in which the European Commission has deemed that the destination provides adequate protection.[6] Over 5,000 companies relied on the E.U.-U.S. Privacy Shield ("Privacy Shield"), which was the prior adequacy decision that facilitated transatlantic transfers.[7] The CJEU struck down that program in *Data Protection Commission v. Facebook Ireland, Schrems*, on the ground that U.S. surveillance programs deprive European data subjects of sufficient protection.[8] The outcome has left international businesses on shaky legal ground when it comes to transfers—the European Data Protection Board has signaled that these transfers can continue, but companies must take

---

[1] David Uberti, *Data-Privacy Impasse Hangs Over U.S.-EU Trade and Technology Summit*, WSJ PRO CYBERSECURITY (Sept. 29, 2021, 4:51 PM), https://www.wsj.com/articles/data-privacy-impasse-hangs-over-u-s-eu-trade-and-technology-summit-11632948689 [https://perma.cc/FC6H-X853].

[2] Karan Bhatia, *The U.S. and Europe Should Launch a Trade and Technology Council*, KEYWORD (Apr. 9, 2021), https://blog.google/outreach-initiatives/public-policy/us-europe-technology-trade-council/ [https://perma.cc/9ZPP-BPZU]; *Chamber Policy Recommendations for the U.S.-EU Trade and Technology Council*, U.S. CHAMBER COM. (Sept. 27, 2021), https://www.uschamber.com/technology/chamber-policy-recommendations-the-us-eu-trade-and-technology-council [https://perma.cc/NX2L-8D5Q].

[3] Commission Regulation 2016/679, General Data Protection Regulation art. 44, 2015 O.J. (L 119) 60.

[4] Commission Regulation 2016/679, General Data Protection Regulation art. 2, 2015 O.J. (L 119) 32; Commission Regulation 2016/679, General Data Protection Regulation art. 3, 2015 O.J. (L 119) 32.

[5] General Data Protection Regulation, *supra* note 3.

[6] Commission Regulation 2016/679, General Data Protection Regulation art. 45, 2015 O.J. (L 119) 61.

[7] Caitlin Fennessy, *The 'Schrems II' Decision: EU-US Data Transfers in Question*, INT'L ASS'N PRIV. PROS. (July 16, 2020), https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/ [https://perma.cc/CLF5-PQUJ].

[8] *Id.*

supplementary security measures in order to avoid penalties.[9] Because no security measures can bridge the gap between government surveillance and GDPR protections, the result is that business communication and data processing have become riskier and more confusing. Unfortunately, the intractable problem that *Schrems* presents will not be solved without a demanding compromise.

In particular, the CJEU took exception to the PRISM and Upstream programs. The CJEU found that through the use of these programs, the United States benefited from "mass processing of personal data without ensuring a level of protection essentially equivalent" to that mandated by E.U. law.[10] In short, U.S. businesses benefited from cross-border data transfers, but the existence of the U.S. government's surveillance programs meant that privacy protection in the U.S. could not meet the GDPR's standard. In addition, the Advocate General[11] noted that E.U. subjects may not enjoy any protection under the Fourth Amendment[12] and that standing[13] and monetary damages requirements in U.S. courts would present substantial obstacles to E.U. citizens seeking to enforce their rights.[14] The Privacy Shield's answer to these problems, the Privacy Shield Ombudsperson,[15] was deemed insufficient to grant adequate protection by the CJEU because the Ombudsperson was not sufficiently independent and did not have the power to constrain the government in any way.[16] In short, the *Schrems* decision makes clear that nothing short of a substantive remedy for unlawful surveillance will be acceptable for a Privacy Shield replacement. From the perspective of the U.S., PRISM and Upstream (the surveillance programs at issue) have withstood years of criticism in the U.S., and even American citizens have had little success in challenging them.[17]

Without a replacement for the Privacy Shield, businesses in the U.S. must resort to other methods, such as employing the E.U.'s Standard Contractual Clauses.[18] However, despite the availability of alternatives, the lack of an easy-to-use framework is causing authorities to advise parties in the E.U. against using services from U.S. providers like Microsoft, Zoom, and Cloudflare, and none of the alternatives address the CJEU's original concern about bulk

---

[9] Catherine Stupp, *European Regulators Continue to Disrupt Data Transfers to U.S.*, WSJ PRO CYBERSECURITY (Sept. 9, 2021, 2:07 PM), https://www.wsj.com/articles/european-regulators-continue-to-disrupt-data-transfers-to-u-s-11630661400 [https://perma.cc/XC9J-6FHJ].

[10] Case C-311/18, Data Prot. Comm'n v. Facebook Ireland, Schrems, ¶ 64 (July 16, 2020), https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=31683147#Footnote* [https://perma.cc/RD9E-8N7A].

[11] The Advocate General is an officer who assists the CJEU. The Advocate General is not a judge but must be similarly qualified. He or she questions the parties and delivers a legal opinion. The CJEU does not always issue a detailed opinion, so the Advocate General's opinion provides the rationale for the court's judgment. This opinion is not binding but provides an important source of legal reasoning and is nonetheless usually followed by the CJEU.

[12] Case C-311/18, Data Prot. Comm'n v. Facebook Ireland, Schrems, ¶ 65 (July 16, 2020), https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=31683147#Footnote* [https://perma.cc/RD9E-8N7A].

[13] *Id.* at ¶¶ 45(115), 65.

[14] *Id.* at ¶ 65.

[15] *Privacy Shield Ombudsperson*, U.S. DEP'T STATE, https://www.state.gov/privacy-shield-ombudsperson/ [https://perma.cc/5BT2-YNJF] (last visited Feb. 6, 2022).

[16] Case C-311/18, Data Prot. Comm'n v. Facebook Ireland, Schrems, ¶¶ 195–96 (July 16, 2020), https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=31683147#Footnote* [https://perma.cc/RD9E-8N7A].

[17] Patrick Toomey, *The NSA Continues to Violate Americans' Internet Privacy Rights*, ACLU (Aug. 22, 2018, 5:30 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy [https://perma.cc/ZE2N-Q3SC]; Jacques Singer-Emery, *The Second Circuit Rules in United States v. Hasbajrami*, LAWFARE (Jan. 7, 2020, 8:00 AM), https://www.lawfareblog.com/second-circuit-rules-united-states-v-hasbajrami [https://perma.cc/58KH-E55T].

[18] Stupp, *supra* note 9.

government surveillance.[19] In order to regain mutual trust and protect data sharing, the Trade and Technology Council must craft a compromise that prioritizes national security while offering data subjects the ability to enforce their rights over the long-term.

Both parties are motivated to find such a compromise. The European Data Protection Board has stated that it is ready to work with the European Commission "to help it build, together with the U.S., a new framework that fully complies with EU data protection law."[20] Nevertheless, it refused to provide an enforcement grace period to allow organizations to continue their transfers, signaling that it would not back down from its insistence on compliance.[21]

The compromise is also highly anticipated by the business community. Jane Horvath, Apple's Chief Privacy Officer, believes that it will take a diverse body of companies pleading the case to Congress to form a solution that benefits everyone, and that solution will take the form of a federal privacy law.[22] Such a law could preempt the complex web of state and sectoral laws that the U.S. currently relies on to police data, making it easier to communicate its needs and abilities to other governments. Alternately, the U.S. could adopt a system like the Asia Pacific Economic Cooperation Cross-Border Privacy Rules, which are based on the idea that privacy frameworks can be interoperable while still diverging according to a jurisdiction's needs.[23] But whatever form the new framework takes, the failure of the original U.S.-E.U. Privacy Shield demonstrates that no jurisdiction will be able to build a functional cross-border data transfer system by striking out on its own, and that careful negotiation is needed to build the trust and understanding necessary for a multilateral solution.

---

[19] *Id.*

[20] *FAQs – EU-U.S. Privacy Shield Program Update*, PRIV. SHIELD FRAMEWORK (Mar. 31, 2021), https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update [https://perma.cc/QT6C-5567].

[21] *Id.*

[22] Joseph Duball, *PSR21 Keynote Stage: Federal Privacy Law Holds the Keys*, INT'L ASS'N PRIV. PROS. (Oct. 22, 2021), https://iapp.org/news/a/psr21-keynote-stage-federal-privacy-law-holds-the-keys/ [https://perma.cc/HAA2-VPME].

[23] Cobun Zweifel-Keegan, *A Globalized CBPR Framework: Peering into the Future of Data Transfers*, INT'L ASS'N PRIV. PROS. (Nov. 23, 2021), https://iapp.org/news/a/a-globalized-cbpr-framework-peering-into-the-future-of-data-transfers/ [https://perma.cc/QJ7U-WNYQ].